<Important Notice>

Apology and Notice Regarding a Personal Information Leak Resulting from Unauthorized Access at Our Outsourcing Partner, Wasabi Co., Ltd.

Published Date: October 24, 2026
Last Updated: October 28, 2026 at 17:00 (JST)

Thank you very much for your continued patronage.

On October 23, we received notification from Wasabi Co., Ltd. (hereinafter “Wasabi”) that “WASABI SWITCH,” the system provided by Wasabi that we use for order management and other purposes at our stores on external marketplaces, had been subject to unauthorized access, resulting in the leakage of our customers’ information.

As of October 22, Wasabi Co., Ltd. had stated that it had “received no reports of a data breach,” but this information has been updated following the progress of Wasabi Co., Ltd.’s forensic investigation.

We sincerely apologize for the significant inconvenience and concern this has caused our customers and all other parties involved.

1. Background

On October 23, 2026, we received a report from Wasabi Inc. regarding a data breach involving our company, based on the results of a reanalysis of logs and a database cross-check.

According to Wasabi Inc.’s records, the breach was first confirmed to have occurred between October 14 and 17, 2026.

*Regarding the data reported as of October 23, it was discovered on October 26 that there was an error in the time specification used by Wasabi Inc. during data extraction; consequently, we have received a revised report on the number of data breaches.

*We have made corrections based on a revised report from Wasabi Co. dated October 27, which corrected the data breach period.
[Before Correction] Between October 14 and 16, 2026
[After Correction] Between October 14 and 17, 2026

Please note that, as of this writing, no unauthorized access has been confirmed in the systems managed by our company.

2. Number of Leaked Records

- Customer order information from external marketplace sites operated by our company: 2,269 records (*An increase of 53 records from the 2,216 reported on October 23)
- Administrative account information: 31 records
- Affected channels: Rakuten Ichiba, eBay, Yahoo! Shopping, Chrono24
- Affected Information: Customer name, phonetic spelling, email address, phone number, address, payment method, total amount, member ID, and administrative account information (administrator ID, login ID, encrypted password)

*The number of records refers to individual orders and does not correspond to the actual number of affected customers.
*Credit card numbers were not included in the leaked information.
*Details regarding the scope of the breach and affected parties are based on Wasabi Inc.'s current investigation and are subject to change depending on the progress of future investigations.

3. Actions Taken to Date and Future Measures

We have promptly reported the incident to the Personal Information Protection Commission and the relevant marketplace operators, and we have changed various passwords and authentication credentials under our management and reviewed access permissions.

Furthermore, since the affected online stores include cross-border e-commerce sites, we are currently confirming whether reports need to be filed with overseas regulatory authorities. In addition, we have requested that Wasabi investigate the cause of the incident and implement measures to prevent a recurrence.

Starting October 28, 2026, we have begun sending individual email notifications to overseas customers whose information was compromised.

4. A Request to Our Customers

If you receive a suspicious email or SMS message purporting to be from our company, an online marketplace, a financial institution, or another entity, please do not click on any URLs and delete the message immediately.

Please note that there has been no leak of your passwords through our company. However, to prevent any potential secondary damage, we recommend that customers who use the same login password across multiple services and websites (such as various online malls and third-party services) change their passwords for security reasons.

Neither our company, Wasabi, nor any external online mall operators will ever ask for your password or credit card information via email or any other means.

Frequently Asked Questions (FAQ)

Q1. Were any credit card details compromised?
A1. Credit card numbers were not included in the compromised data.

Q2. What information may have been compromised?
A2. Customer order information (2,269 records), including the customer's name, phonetic spelling, email address, phone number, address, payment method, total amount, and member ID.
*Please note that we have updated the number of affected records because it was discovered that there was an error in the time specified by Wasabi Inc. during data extraction.

Additionally, the following information from administrative account records (31 records) was compromised: administrator ID, login ID, and encrypted passwords.
Please note that the number of order records refers to individual orders and does not correspond to the actual number of people.

Q3. Can I check if my information was leaked?
A3. Details regarding the scope and targets of the leak are based on Wasabi Inc.'s current investigation and are subject to change depending on the progress of future investigations. For further details, please contact the inquiry desk listed below or check the dedicated information page provided by Wasabi Inc., our contracted service provider.

Q4. What should I do if I receive suspicious communication?
A4. Please be aware that these may be emails, phone calls, or text messages (SMS) pretending to be from our company. If you receive any suspicious communications, please contact our Personal Information Consultation Desk.

Q5. Did our company's own systems also suffer unauthorized access?
A5. As of now, we have not confirmed any unauthorized access to the systems under our management. This data breach resulted from unauthorized access to Wasabi Inc.'s "WASABI SWITCH" system, which is used for order management and other purposes by our external online mall stores.

Q6. Were registration data from the websites we operate—"MapCamera.com," "GMT.com," "BRILLER-GMT.com," and "KINGDOM NOTE.com"—also leaked?
A6. The affected data all pertain to our external marketplace stores. We do not use "WASABI SWITCH" for order management on the websites we operate, so there is no connection to this incident.

Q7. Please provide an update on the status of the external marketplace stores that are currently suspended as part of WASABI's security response to the unauthorized access incident.
A7. As of October 25, 2026, operations at the following stores have been temporarily suspended:
・Map Camera Rakuten Ichiba Store

・Map Camera eBay Store
・GMT Rakuten Ichiba Store
・BRILLER Rakuten Ichiba Store
・Yahoo! Shopping GMT Watch Specialty Store
・GMT eBay Store
・Chrono24 GMT

Please note that since the websites operated by our company do not use “WASABI SWITCH,”
They remain open for business.

Contact Information Regarding This Matter

■ Shuppin Co., Ltd. Personal Information Inquiry Desk
Email Address: privacy@syuppin.com
Hours: 24 hours a day *We will respond in the order inquiries are received, but please note that it may take some time depending on the volume of inquiries.

■ Wasabi Co., Ltd. (Contractor) Special Support Desk & Information
For detailed information regarding the status of the investigation into this incident and the system-side measures being taken, please also refer to the dedicated page and support desk set up by Wasabi Co., Ltd. below.

Information Page for Purchasers: https://incident-support.wasabi-inc.biz/customers
Inquiry Desk (Web Form): https://incident-support.wasabi-inc.biz/contact#customer
*We are currently accepting inquiries via the dedicated web form. Please note that we are in the process of preparing and launching a dedicated call center.

We will promptly report any progress in the investigation or new developments as they arise.